Security or Privacy Breach
Frequently Asked Questions

1. What is a security or privacy breach?

A security or privacy breach any real or suspected adverse event whereby some aspect of security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.

A privacy breach is an unauthorized disclosure of protected health information (PHI)/personal confidential information (PCI) that violates either federal or state laws

- Federal: HIPAA Privacy Rule
- State: Information Practices Act of 1977

Security or privacy breaches may be paper or electronic. If breach involves computerized information that is unencrypted; including name, Social Security number, DMV or financial account information, then breach triggers the state breach notification law.

2. What are some examples of security or privacy breaches that involve paper?

- Misdirected paper faxes with PHI/PCI outside of CDHS
- Loss or theft of paper documents containing PHI/PCI
- Mailings to incorrect providers or beneficiaries

3. What are some examples of electronic security or privacy breaches?

- Stolen, unencrypted laptops, hard drives, PCs with PHI/PCI
- Stolen, unencrypted thumb drives with PHI/PCI
- Stolen briefcases with unencrypted compact discs containing PHI/PCI
- Misdirected electronic fax with PHI/PCI to person outside of state government

4. If some of my information is stolen or otherwise involved in a security or privacy breach, does this mean that I'm a victim of identity theft?

No, this does not mean that you are a victim of identity theft! The fact that some of your information may have been involved in a privacy breach does not mean that a person attempted to or did access your information or that your information has been used inappropriately. The way to protect yourself is to place a fraud alert on your credit files and review your credit reports.

5. How will I know if any of my personal information was used by someone else?

The best way to find out is to order your credit reports from the three credit bureaus: Equifax, Experian and Trans Union. If you notice accounts on your credit report that you did not open or applications for credit ("inquiries") that you did not make, these could be indications that someone else is using your personal information, without your permission.

6. What can I do to protect myself?

You may do two things, both of which are free. First, you can look at your credit report to ensure that no new accounts in your name have been established. Second, you can place a "fraud alert" on your credit report to ensure that no one will be able to easily establish credit in your name.

7. Do I have to pay for the credit report?

As a possible fraud victim, you are entitled to a free copy of your credit report. Simply call any one of the three credit bureaus at the numbers provided and follow the "fraud victim" instructions. You will automatically place a fraud alert on your credit file with all three of the bureaus. Experian allows you to file a fraud alert online also.

Experian
http://www.experian.com
Online fraud alert: http://www.experian.com/consumer/fraud_faqs.html
(888) 397-3742

Equifax
http://www.equifax.com
(800) 525-6285

TransUnion
http://www.transunion.com
(800) 680-7289

You will soon receive a letter from each bureau confirming the fraud alert and telling you how to order a free copy of your credit report. Follow the instructions in the letters to receive your free reports.

(Note: This free credit report that you're entitled to as a potential fraud victim is in addition to the free annual report that everyone is now entitled to. See www.privacy.ca.gov for more info on the free annual report.)

8. I called the credit bureau fraud line and they asked for my Social Security Number. Is it okay to give it?

The credit bureaus ask for your Social Security number and other information in order to identify you and avoid sending your credit report to the wrong person. It is okay to give this information to the credit bureau that you call.

9. Why can't I talk to someone at the credit bureaus?

You must first order your credit reports. When you receive your reports, each one will have a phone number you can call to speak with a live person in the bureau's fraud unit. If you see anything on any of your reports that looks unusual or that you don't understand, call the number on the report.

10. Can I file my fraud alert online?

Experian allows you to file a fraud alert online
http://www.experian.com/consumer/fraud_faqs.html

11. Can I get my free credit report online?

If you have a computer with Internet access, you can obtain a free report instantly. For the free report from any one or all of the three credit bureaus, do not go directly to the credit bureau websites, as they will try to charge you for this service. Use this link: http://www.annualcreditreport.com

12. Do I have to call all three credit bureaus?

No. If you call just one of the bureaus, they will notify the other two. A fraud alert will be placed on your file with all three and you will receive a confirming letter from all three.

13. What is a fraud alert?

A fraud alert is a message that credit issuers receive when someone applies for new credit in your name. The message tells creditors that there is possible fraud associated with the account and gives them a phone number to call (yours) before issuing new credit. When you call the credit bureau fraud line, you will be asked for identifying information and will be given the opportunity to enter a phone number for creditors to call. You may want to make this your cell phone number.

14. Will my credit be affected by filing a "Fraud Alert"?

Putting a "Fraud Alert" on your credit report will not harm your credit. The presence of a fraud alert should not interfere with your daily use of a credit card or banking/checking accounts. A fraud alert may limit your ability to obtain instant credit for immediate, in-store purchases. If you prefer to purchase items on a new line of credit (that is, a new credit card) at a retail store and you want to buy those items immediately, your request for credit may be delayed because of the fraud alert placed on your credit.

15. Will a fraud alert stop me from using my credit cards?

No. A fraud alert will not stop you from using your existing credit cards or other accounts. It may slow down your ability to get *new* credit. Its purpose is to help protect you against an identity thief trying to open credit accounts in your name. Credit issuers get a special message alerting them to the possibility of fraud. Creditors know that they should take "reasonable steps" to re-verify the identity of the person applying for credit.

16. How long does a fraud alert last?

An initial fraud alert lasts 90 days. You can remove an alert by calling the credit bureaus at the phone number given on your credit report. If you want to reinstate the alert, you can also do so.

17. How long does it take to receive my credit report?

It could take about 20 days from the day you call the credit bureaus. It takes about 5 to 10 days from the time you call the credit bureaus to get your fraud alert confirmation letter with instructions on ordering your credit report. You should receive your reports in another 5 to 10 days from the time you order them.

18. What should I look for on my credit report?

Look for any accounts that you don't recognize, especially accounts opened recently. Look at the inquiries or requests section for names of creditors from whom you haven't requested credit. Note that some kinds of inquiries, labeled something like "promotional inquiries," are for unsolicited offers of credit, mostly from companies with whom you do business.

Don't be concerned about those inquiries as a sign of fraud. (You are automatically removed from lists to receive unsolicited pre-approved credit offers when you put a fraud alert on your account. You can also stop those offers by calling 888-5OPTOUT.)

Look in the personal information section for addresses where you've never lived. Any of these things might be indications of fraud. Also be on the alert for other possible signs of identity

theft, such as calls from creditors or debt collectors about bills that you don't recognize, or unusual charges on your credit card bills.

19. How often should I order new credit reports and how long should I go on ordering them?

It might be a good idea to order copies of your credit reports every three months for a while. How long you continue to order them is up to you. Identity thieves usually, but not always, act soon after stealing personal information. We recommend checking your credit reports at least twice a year as a general privacy protection measure.

20. Should I contact the Social Security Administration and change my Social Security number?

The Social Security Administration very rarely changes a person's SSN. And the mere possibility of fraudulent use of your SSN would probably not be viewed as a justification. There are drawbacks to doing so. The absence of any history under the new SSN would make it difficult to get credit, continue college, rent an apartment, open a bank account, get health insurance, etc. In most cases, getting a new SSN would not be a good idea.

21. Should I close my bank account?

No, not unless your bank account number was among the items of personal information compromised in the breach. (As a general privacy protection measure, you should limit the use of your SSN where it's not required. For example, if your bank account number or PIN is your SSN, you should ask the bank to give you a different number. Do NOT use last four digits of your SSN, your mother's maiden name or your birth date as a password for financial transactions.)

22. Should I close my credit card or other accounts?

No, not unless your account number was among the items of personal information compromised in the breach. (As a general privacy protection measure, you should always look over your credit card bills carefully to see if there are any purchases you didn't make. If so, contact the card company immediately.)

23. What happens if I find out that I have been a victim of identify theft?

If you find evidence of identity theft on your credit reports, take these steps:

- Close the credit card accounts that you believe have been opened fraudulently or have unauthorized activity.
- File a report with your local police department, and get a copy to submit to creditors and others that may require proof of a crime.
- Contact the credit bureaus to place a victim statement on your account.
- File a complaint with the FTC online (http://www.consumer.gov/idtheft) or by calling (877) 438-4338.
- If you discover misuse of your Social Security number, call the Social Security Fraud Hotline, (800) 269-0271.
- Keep a record of communications with credit bureaus, creditors, financial institutions, and police, including dates.

For more information on what to do, see the Identity Theft Victim Checklist on the Identity Theft page of the California Office of Privacy Protection's Web site at **www.privacy.ca.gov**.

24. What if I have a fraud alert on, but I want to apply for credit?

You should still be able to get credit. While a fraud alert may slow down the application process, you can prove your identity to a prospective creditor by providing identifying information.

25. I heard that I could "freeze" my credit files. How does that work?

A security freeze is a stronger measure than a fraud alert. A freeze prevents others from seeing your credit history without your permission. Unlike the fraud alert that lasts 90 days, a credit freeze remains in effect until such time as the consumer elects to terminate the freeze. It costs $10 to place a freeze with each of the three credit bureaus, for a total cost of $30. You can also temporarily lift the freeze for $10, if you want to apply for new credit yourself. For more information on the freeze, see the Identity Theft page of the Office of Privacy Protection's Web site: http://www.privacy.ca.gov/cover/identitytheft.htm. (If no Internet access, they can call the California Office of Privacy Protection at 866-785-9663.)

26. The notice is addressed to my spouse, who is deceased. What should I do?

Call each of the credit bureaus at the numbers in the notice letter. Follow the fraud cues and enter the deceased person's information. If you get a message that says "reported deceased" or "no report on file" or something like that, that's good. That means the credit bureaus have been notified by the Social Security Administration that the holder of the SSN is deceased. (Counties notify SSA when a death certificate is filed. The whole process can take months.) A creditor doing a credit check would get the same message, pretty much eliminating the risk of new credit being established in the person's name/number.

If the fraud alert process on the automated phone system goes through, that may mean that the credit bureaus haven't been notified of the death. In that case the spouse (or the executor of the estate) should notify the credit bureaus in writing that the person is deceased and that the person's information may be at risk of identity theft. The credit bureaus will flag the file as deceased. The spouse (or executor) must include the following information in the letters to the credit bureaus:

- Deceased's full name, date of birth, most recent address, and SSN
- Copy of the death certificate
- The spouse may request and receive a copy of the deceased's credit report at the spouse's home address.
- An executor wishing to receive a copy of the deceased's credit report should enclose a copy of the executorship papers.

27. The notice is addressed to my child, who is a minor. What should I do?

Call each of the credit bureaus at the numbers in the notice letter. Follow the fraud cues on the automated system and enter the child's information. If you get a message of "report not found" or something like that, that's good. That means your child doesn't have a credit history. A creditor doing a credit check would get the same message, pretty much eliminating the risk of new credit being established in the child's name. You might go through this process every few months for six months to a year.

If the fraud alert process goes through, then you'll get a confirming letter in the mail from each of the credit bureaus with instructions for ordering your child's credit report. Check the report(s) and call the credit bureaus about any information that looks suspicious or inaccurate.

28. What are the addresses of the Credit Bureaus?

Mail to the credit bureau addresses below.

Credit Bureau Fraud Departments

	Experian	Trans Union	Equifax
Phone	888-397-3742	800-680-728	800-525-628
TDD	800-972-0322	877-553-7803	1-800-255-0056 & ask for Auto Disclosure Line, 800-685-1111
Address	P.O. Box 9532 Allen, TX 75013	P.O. Box 6790 Fullerton, CA 92834	P.O. Box 740241 Atlanta, GA 30374-0241
Website	www.experian.com	www.transunion.com	www.equifax.com

29. Are there other resources available to me?

A. California Office of Privacy Protection
http://privacy.ca.gov/cover/identitytheft.htm
http://privacy.ca.gov/cover/consumerinfo.htm
This division of the state Department of Consumer Affairs offers a variety of information and services related to identity theft, including prevention tips.

B. California Attorney General's Office
http://caag.state.ca.us/idtheft/index.htm
The Attorney General's Office maintains an Identity Theft Registry and gives information about investigation and prosecution of identity-theft crimes.

C. Social Security Administration
http://www.ssa.gov/pubs/idtheft.htm
The Social Security Administration gives information on how to report the fraudulent use of a Social Security card and how to correct your earnings record.

D. Federal Trade Commission
http://www.ftc.gov/bcp/edu/microsites/idtheft/
This is the main U.S. government site for identity-theft information. The FTC also maintains a database of identity theft cases used by law enforcement agencies for investigations.

E. Privacy Rights Clearing House
http://www.privacyrights.org/identity.htm
Find statistics, fact sheets, and government records about identity theft.

F. Identity Theft Resource Center
http://www.idtheftcenter.org
This nonprofit organization provides consumer alerts, scam warnings, and instructions for victims of identity theft.